CLAIMS

What is claimed is:

1. A method for applying a service to an encrypted packet comprising:
examining an encrypted packet;
determining whether an identifier associated with the service is present in the encrypted packet;
if it is determined that the identifier is present in the encrypted packet, applying the service to the encrypted packet.

2. The method of claim 1, further comprising the steps of:
encrypting the packet, wherein said step of encryption includes establishing said identifier in the packet.

3. The method of claim 1, wherein said identifier is based on at least on an Internet Key Exchange (IKE) ID stored in the packet.

4. The method of claim 3, wherein the Internet Key Exchange (IKE) ID comprises one or more of ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, and ID_KEY_ID.

5. The method of claim 1, wherein the identifier is based on at least an entry in a security association database.

6. The method of claim 1, wherein said identifier maps to quality of service (QoS) group.

7. The method of claim 2, wherein the identifier is established in a profile of the packet.

8. The method of claim 7, wherein the profile is an ISAKMP profile.

9. The method of claim 2, further comprising a step of pre-classification of the packet prior to the step of encryption.

10. The method of claim 9, wherein the service that is applied is selected based on both the identifier and pre-classification.

11. A method for applying a service to a packet comprising:
encrypting the packet to create an encrypted packet;
examining an identifier in the encrypted packet, wherein the identifier is based on an IKE ID of the encrypted packet;
determining whether the identifier in the encrypted packet is associated with a service to be applied to the encrypted packet; and
if it is determined that the identifier is associated with a service to be applied to the encrypted packet, applying the service to the encrypted packet.

12. The method of claim 11, further comprising the step of:
prior to the step of encrypting, pre-classifying the packet based on the contents of the packet;
wherein the service that is applied to the packet is selected partially based the step of pre-classification and partially based on the identifier.

13. The method of claim 11, further comprising the step of:
during encryption, copying at least one bit into a header to identify a characteristic of the packet;
wherein the service that is applied to the packet is selected partially based on a value of the at least one bit and partially based on the identifier.

14. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 1.

15. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 2.

16. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 3.

17. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 4.

18. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 5.

19. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 6.

20. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 7.

21. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 8.

22. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 9.

23. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 10.

24. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 11.

25. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 12.

26. A computer-readable medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out the steps recited in claim 13.

27. An apparatus for applying a service to an encrypted packet comprising:
means for examining an encrypted packet;
means for determining whether an identifier associated with the service is present in the encrypted packet;

means for applying the service to the encrypted packet if it is determined that the identifier is present in the encrypted packet.

28. The apparatus of claim 27, further comprising means for encrypting the packet, wherein the means for encryption includes means for establishing said identifier in the packet.

29. The apparatus of claim 27, wherein said identifier is based on at least on an Internet Key Exchange (IKE) ID stored in the packet.

30. The apparatus of claim 29, wherein the Internet Key Exchange (IKE) ID comprises one or more of ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, and ID_KEY_ID.

31. The apparatus of claim 27, wherein the identifier is based on at least an entry in a security association database.

32. The apparatus of claim 27, wherein said identifier maps to quality of service (QoS) group.

33. The method of claim 2, wherein the identifier is established in a profile of the packet.

34. The method of claim 7, wherein the profile is an ISAKMP profile.

35. The method of claim 2, further comprising means for pre-classification of the packet prior to the step of encryption.

36. The method of claim 9, wherein the service that is applied is selected based on both the identifier and pre-classification.

37. An apparatus for applying a service to an encrypted packet comprising:
one or more processors;
memory communicatively coupled to the one or more processors;
one or more sequences of instructions in the memory for applying a service to an encrypted packet, which instructions, when executed by the one or more processors, cause the one or more processors to perform the steps of:
examining an encrypted packet;
determining whether an identifier associated with the service is present in the encrypted packet;
if it is determined that the identifier is present in the encrypted packet, applying the service to the encrypted packet.

38. The apparatus of claim 37, further comprising sequences of instructions for performing the steps of:
encrypting the packet, wherein said step of encryption includes establishing said identifier in the packet.

39. The apparatus of claim 37, wherein said identifier is based on at least on an Internet Key Exchange (IKE) ID stored in the packet.

40. The apparatus of claim 39, wherein the Internet Key Exchange (IKE) ID comprises one or more of ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, and ID_KEY_ID.

41. The apparatus of claim 37, wherein the identifier is based on at least an entry in a security association database.

42. The apparatus of claim 37, wherein said identifier maps to quality of service (QoS) group.

43. The apparatus of claim 38, wherein the identifier is established in a profile of the packet.

44. The apparatus of claim 43, wherein the profile is an ISAKMP profile.

45. The apparatus of claim 38, further comprising a step of pre-classification of the packet prior to the step of encryption.

46. The apparatus of claim 45, wherein the service that is applied is selected based on both the identifier and pre-classification.